vulnerabilities, and the cost to a computer facility or word processing activity in safeguarding personal information processed or stored in the facility or activity.

(o) *Routine use.* The disclosure of a record outside DoD for a use that is compatible with the purpose for which the information was collected and maintained by DoD. The routine use must be included in the published system notice for the system of records involved.

(p) *Statistical record.* A record maintained only for statistical research or reporting purposes and not used in whole or in part in making determinations about specific individuals.

(q) *System of Records.* A group of records under the control of a DLA activity from which information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to the individual. System notices for all Privacy Act systems of records must be published in the FEDERAL REGISTER.

§ 323.4 Responsibilities.

(a) Headquarters Defense Logistics Agency.

(1) The Staff Director, Corporate Communications, DLA Support Services (DSS-C) will:

(i) Formulate policies, procedures, and standards necessary for uniform compliance with the Privacy Act by DLA activities.

(ii) Serve as the DLA Privacy Act Officer and DLA representative on the Defense Privacy Board.

(iii) Maintain a master registry of system notices published by DLA.

(iv) Develop or compile the rules, notices, and reports required under this part.

(v) Establish training programs for all individuals with public affairs duties, and all other personnel whose duties require access to or contact with systems of records affected by the Privacy Act. Initial training will be given to new employees and military members upon assignment. Refresher training will be provided annually or more frequently if conditions warrant.

(2) The General Counsel, DLA (DLA-GC) will:

(i) Serve as the appellate authority for denials of individual access and amendment of records.

(ii) Provide representation to the Defense Privacy Board Legal Committee.

(iii) Advise the Defense Privacy Office on the status of DLA privacy litigation.

(3) The DLA Chief Information Office (J–6) will formulate and implement protective standards for personal information maintained in automated data processing systems and facilities.

(b) The Heads of DLA Primary Level Field Activities (PLFAs) will:

(1) Ensure that the collection, maintenance, use, or dissemination of records of identifiable personal information is in a manner that assures that such action is for a necessary and lawful purpose; that the information is timely and accurate for its intended use; and that adequate safeguards are provided to prevent misuse of such information.

(2) Designate a Privacy Act Officer to serve as the principal point of contact on privacy matters.

(3) Ensure the internal operating procedures provide for effective compliance with the Privacy Act.

(4) Establish training programs for all individuals with public affairs duties, and all other personnel whose duties require access to or contact with systems of records affected by the Privacy Act. Initial training will be given to new employees and military members upon assignment. Refresher training will be provided annually or more frequently if conditions warrant.

[DLAR 5400.21, 51 FR 33595, Sept. 22, 1986, unless otherwise noted. Redesignated at 56 FR 57803, Nov. 14, 1991, as amended at 66 FR 41781, Aug. 9, 2001]

§ 323.5 Procedures.

(a) *Individual access.* (1) The access provisions of this part are intended for use by individuals whose records are maintained in systems of records. Release of personal information to individuals under this part is not considered public release of information.

(2) Individuals will address requests for access to personal information about themselves in a system of records to the system manager or to

the office designated in the system notice. Before being granted access to personal data, an individual may be required to provide reasonable verification of his or her identity. Identity verification procedures will be simple so as not to discourage individuals from seeking access to information about themselves; or be required of an individual seeking access to records which normally would be available under 32 CFR part 1285 (DLAR 5400.14).

(i) Normally, when individuals seek personal access to records pertaining to themselves, identification will be made from documents that normally are readily available, such as employee and military identification cards, driver's license, other licenses, permits, or passes used for routine identification purposes.

(ii) When access is requested by mail, identity verification may consist of the individual providing certain minimum identifying data, such as full name, date and place of birth, or such other personal information necessary to locate the record sought. If the information sought is sensitive, additional identifying data may be required. If notarization of requests is required, procedures will be established for an alternate method of verification for individuals who do not have access to notary services, such as military members overseas.

(3) If an individual wishes to be accompanied by a third party when seeking access to his or her records or to have the records released directly to a third party, the individual may be required to furnish a signed access authorization granting the third party access. An individual will not be refused access to his or her record solely for failure to divulge his or her social security number (SSN) unless it is the only method by which retrieval can be made. The individual is not required to explain or justify his or her need for access to any record under this part.

(4) Disclose medical records to the individual to whom they pertain, even if a minor, unless a judgment is made that access to such records could have an adverse effect on the mental or physical health of the individual. Normally, this determination will be made in consultation with a medical doctor. If it is determined that the release of the medical information may be harmful to the mental or physical health of the individual, send the record to a physician named by the individual and in the transmittal letter to the physician, explain why access by the individual without proper professional supervision could be harmful (unless it is obvious from the record). Do not require the physician to request the records for the individual. If the individual refuses or fails to designate a physician, the record will not be provided. Such refusal of access is not considered a denial for reporting purposes.

(5) Requests by individuals for access to investigatory records pertaining to themselves and compiled for law enforcement purposes are processed under this part or 32 CFR part 1285 depending on which part gives them the greatest degree of access.

(6) Certain documents under the physical control of DoD personnel and used to assist them in performing official functions, are not considered ''agency records'' within the meaning of this part. Uncirculated personal notes and records that are not disseminated or circulated to any person or organization (for example, personal telephone lists or memory aids) that are retained or discarded at the author's discretion and over which DLA exercises no direct control, are not considered agency records. However, if personnel are officially directed or encouraged, either in writing or orally, to maintain such records, they may become ''agency records,'' and may be subject to the Privacy Act of 1974 (5 U.S.C. 552a) and this part.

(7) Acknowledge requests for access within 10 working days after receipt and provide access within 30 working days.

(b) *Denial of individual access.* (1) Individuals may be formally denied access to a record pertaining to them only if the record was compiled in reasonable anticipation of civil action; is in a system of records that has been exempted from the access provisions of this part under one of the permitted exemptions; contains classified information that has been exempted from the access provision of this part under the blanket

exemption for such material claimed for all DoD records systems; or is contained in a system of records for which access may be denied under some other Federal statute. Only deny the individual access to those portions of the records from which the denial of access serves some legitimate Governmental purpose.

(2) An individual may be refused access if the record is not described well enough to enable it to be located with a reasonable amount of effort on the part of an employee familiar with the file; or access is sought by an individual who fails or refuses to comply with the established procedural requirements, including refusing to name a physician to receive medical records when required or to pay fees. Always explain to the individual the specific reason access has been refused and how he or she may obtain access.

(3) Formal denials of access must be in writing and include as a minimum:

(i) The name, title or position, and signature of the appropriate Head of the HQ DLA principal staff element or primary level field activity.

(ii) The date of the denial.

(iii) The specific reason for the denial, including specific citation to the appropriate sections of the Privacy Act of 1974 (5 U.S.C. 552a) or other statutes, this part, or DLAR 5400.21 authorizing the denial.

(iv) Notice to the individual of his or her right to appeal the denial within 60 calendar days of the date of the denial letter and to file any such appeal with the HQ DLA Privacy Act Officer, Defense Logistics Agency (DSS-CA), 8725 John J. Kingman Road, Suite 2533, Fort Belvoir, VA 22060–6221.

(4) DLA will process all appeals within 30 days of receipt unless a fair an equitable review cannot be made within that period. The written appeal notification granting or denying access is the final DLA action on access.

(5) The records in all systems of records maintained in accordance with the Office of Personnel Management (OPM) Government-wide system notices are technically only in the temporary custody of DLA. All requests for access to these records must be processed in accordance with the Federal Personnel Manual (5 CFR parts 293, 294, 297 and 735) as well as this part. DLA–GC is responsible for the appellate review of denial of access to such records.

(c) *Amendment of records.* (1) Individuals are encouraged to review the personal information being maintained about them by DLA and to avail themselves of the procedures established by this part to update their records. An individual may request the amendment of any record contained in a system of records pertaining to him or her unless the system of record has been exempted specifically from the amendment procedures of this part. Normally, amendments under this part are limited to correcting factual matters and not matters of official judgment, such as performance ratings promotion potential, and job performance appraisals.

(2) The applicant must adequately support his or her claim and may be required to provide identification to ensure that they are indeed seeking to amend a record pertaining to themselves and not, inadvertently or intentionally, the record of others. Consider the following factors when evaluating the sufficiency of a request to amend:

(i) The accuracy of the information itself.

(ii) The relevancy, timeliness, completeness, and necessity of the recorded information for accomplishing an assigned mission or purpose.

(3) Provide written acknowledgement of a request to amend within 10 working days of its receipt by the appropriate systems manager. There is no need to acknowledge a request if the action is completed within 10 working days and the individual is so informed. The letter of acknowledgement shall clearly identify the request and advise the individual when he or she may expect to be notified of the completed action. Only under the most exceptional circumstances will more than 30 days be required to reach a decision on a request to amend.

(4) If the decision is made to grant all or part of the request for amendment, amend the record accordingly and notify the requester. Notify all previous recipients of the information, as reflected in the disclosure accounting records, that an amendment has been

made and the substance of the amendment. Recipients who are known to be no longer retaining the information need not be advised of the amendment. All DoD Components and Federal agencies known to be retaining the record or information, even if not reflected in disclosure records, will be notified of the amendment. Advise the requester of these notifications, and honor all requests by the requester to notify specific Federal agencies of the amendment action.

(5) If the request for amendment is denied in whole or in part, promptly advise the individual in writing of the decision to include:

(i) The specific reason and authority for not amending.

(ii) Notification that he or she may seek further independent review of the decision by filing an appeal with the HQ DLA Privacy Act Officer, Defense Logistics Agency (DSS-CA), 8725 John J. Kingman Road, Suite 2533, Fort Belvoir, VA 22060–6221, and including all supporting materials.

(6) DLA will process all appeals within 30 days unless a fair review cannot be made within this time limit.

(i) If the appeal is granted, DLA will promptly notify the requester and system manager of the decision. The system manager will amend the record(s) as directed and ensure that all prior known recipients of the records who are known to be retaining the record are notified of the decision and the specific nature of the amendment and that the requester is notified as to which DoD Components and Federal agencies have been told of the amendment.

(ii) If the appeal is denied completely or in part, the individual is notified in writing by the reviewing official that:

(A) The appeal has been denied and the specific reason and authority for the denial.

(B) The individual may file a statement of disagreement with the appropriate authority and the procedures for filing this statement.

(C) If filed properly, the statement of disagreement shall be included in the records, furnished to all future recipients of the records, and provided to all prior recipients of the disputed records who are known to hold the record.

(D) The individual may seek a judicial review of the decision not to amend.

(7) The records in all systems of records controlled by the Office of Personnel Management (OPM) Government-wide system notices are technically only temporarily in the custody of DLA. All requests for amendment of these records must be processed in accordance with the Federal Personnel Manual (FPM). A DLA denial authority may deny a request. However, the appeal process for all such denials must include a review by the Assistant Director for Agency Compliance and Evaluation, Office of Personnel Management, 1900 E Street, NW., Washington, DC 20415. When an appeal is received from a DLA denial of amendment of the OPM controlled record, process the appeal in accordance with the FPM and notify the OPM appeal authority listed above. The individual may appeal any DLA decision not to amend the OPM records directly to OPM. OPM is the final review authority for any appeal from a denial to amend the OPM records.

(8) If the reviewing authority refuses to amend the record as requested, the individual may submit a concise statement of disagreement setting forth his or her reasons for disagreeing with the decision not to amend.

(i) If an individual chooses to file a statement of disagreement, annotate the record to indicate that the statement has been filed. Furnish copies of the statement of disagreement to all DoD Components and Federal agencies that have been provided copies of the disputed information and who may be maintaining the information.

(ii) When possible, incorporate the statement of disagreement into the record. If the statement cannot be made a part of the record, establish procedures to ensure that it is apparent from the records that a statement of disagreement has been filed and maintain the statement so that it can be obtained readily when the disputed information is used or disclosed. Automated record systems that are not programmed to accept statements of disagreement shall be annotated or coded so that they clearly indicate that a statement of disagreement is on file,

and clearly identify the statement with the disputed information in the system. Provide a copy of the statement of disagreement whenever the disputed information is disclosed for any purpose.

(9) A summary of reasons for refusing to amend may be included with any record for which a statement of disagreement is filed. Include in this summary only the reasons furnished to the individual for not amending the record. Do not include comments on the statement of disagreement. Normally, the summary and statement of disagreement are filed together. When disclosing information for which a summary has been filed, a copy of the summary may be included in the release, if desired.

(d) *Documentation.* Establish a separate Privacy Case File to retain the documentation received and generated during the amendment or access process. There is no need to establish a Privacy Case File if the individual has not cited the Privacy Act or this part. Privacy Case Files shall not be furnished or disclosed to anyone for use in making any determination about the individual other than determinations made under this part. Only the items listed below may be included in the system of records challenged for amendment or for which access is sought. Do not retain copies of unamended records in the basis record system if the request for amendment is granted.

(1) The following items relating to an amendment request may be included in the disputed record system:

(i) Copies of the amended record.

(ii) Copies of the individual's statement of disagreement.

(iii) Copies of activity summaries.

(iv) Supporting documentation submitted by the individual.

(2) The following items relating to an access request may be included in the basic records system:

(i) Copies of the request.

(ii) Copies of the activity action granting total access. (Note: A separate Privacy Case File need not be created in such cases.)

(iii) Copies of the activity action denying access.

(iv) Copies of any appeals filed.

(v) Copies of the reply to the appeal.

(e) *Fees.* An individual may be charged only for the direct cost of copying and reproduction, computed using the appropriate portions of the fee schedule in DLAR 5400.14 (32 CFR part 1285) under the provisions of this part. Normally, fees are waived automatically if the direct costs of a given request is less than $30. This fee waiver provision does not apply when a waiver has been granted to the individual before, and later requests appear to be an extension or duplication of that original request. DLA activities may, however, set aside this automatic fee waiver provision when on the basis of good evidence it determines that the waiver of fees is not in the public interest. Decisions to waive or reduce fees that exceed the automatic waiver threshold will be made on a case-by-case basis. Fees may not be charged when:

(1) Copying is performed for the convenience of the Government or is the only means to make the record available to the individual.

(2) The record may be obtained without charge under any other part, directive, or statute.

(3) Providing documents to members of Congress for copying records furnished even when the records are requested under the Privacy Act on behalf of a constituent.

(f) *Disclosures of personal information.* (1) For the purposes of disclosure and disclosure accounting, the Department of Defense is considered a single agency. Records pertaining to an individual may be disclosed without the consent of the individual to any DoD official who has need for the record in the performance of his or her assigned duties. Do not disclose personnel information from a system of records outside the Department of Defense unless the record has been requested by the individual to whom it pertains; the written consent of the individual to whom the record pertains has been obtained for release of the record to the requesting agency, activity, or individual; or the release is for one of the specific nonconsensual purposes set forth in this part or DLAR 5400.14, (32 CFR part 1285).

(2) Except for releases made in accordance with DLAR 5400.14, (32 CFR

part 1285) before disclosing any personal information to any recipient outside DoD other than a Federal agency or the individual to whom it pertains;

(i) Ensure that the records are accurate, timely, complete, and relevant for agency purposes.

(ii) Contact the individual, if reasonably available, to verify the accuracy, timeliness, completeness, and relevancy of the information, if this cannot be determined from the record.

(iii) If the information is not current and the individual is not reasonably available, advise the recipient that the information is believed accurate as of a specific date and any other known factors bearing on its accuracy and relevancy.

(3) All records must be disclosed if their release is required by the Freedom of Information Act. DLAR 5400.14, (32 CFR part 1285) requires that records be made available to the public unless exempted from disclosure by one of the nine exemptions found in the Freedom of Information Act. The standard for exempting most personal records, such as personnel records, medical records, and similar records, is found in DLAR 5400.14 (32 CFR part 1285). Under the exemption, release of personal information can only be denied when its release would be a 'clearly unwarranted invasion of personal privacy.'

(i) All disclosures of personal information regarding Federal civilian employees will be made in accordance with the Federal Personnel Manual. Some examples of personal information regarding DoD civilian employees that normally may be released without a clearly unwarranted invasion of personal privacy include:

(A) Name.

(B) Present and past position titles.

(C) Present and past grades.

(D) Present and past salaries.

(E) Present and past duty stations.

(F) Office and duty telephone numbers.

(ii) All release of personal information regarding military members shall be made in accordance with the standards established by DLAR 5400.14, (32 CFR part 1285). While it is not possible to identify categorically information that must be released or withheld from military personnel records in every instance, the following items of personal information regarding military members normally may be disclosed without a clearly unwarranted invasion of their personal privacy:

(A) Full name.

(B) Rank.

(C) Date of rank.

(D) Gross salary.

(E) Past duty assignments.

(F) Present duty assignment.

(G) Future assignments that are officially established.

(H) Office or duty telephone numbers.

(I) Source of commission.

(J) Promotion sequence number.

(K) Awards and decorations.

(L) Attendance at professional military schools.

(M) Duty status at any given time.

(iii) All releases of personal information regarding civilian personnel not subject to the FPM shall be made in accordance with the standards established by DLAR 5400.14 (32 CFR part 1285). While it is not possible to identify categorically those items of personal information that must be released regarding civilian employees not subject to the FPM, such as nonappropriated fund employees, normally the following items may be released without a clearly unwarranted invasion of personal privacy:

(A) Full name.

(B) Grade or position.

(C) Date of grade.

(D) Gross salary.

(E) Present and past assignments.

(F) Future assignments, if officially established.

(G) Office or duty telephone numbers.

(4) A request for a home address or telephone number may be referred to the last known address of the individual for a direct reply by him or her to the requester. In such cases the requester will be notified of the referral. The release of home addresses and home telephone numbers normally is considered a clearly unwarranted invasion of personal privacy and is prohibited. However, these may be released without prior specific consent of the individual if:

(i) The individual has indicated previously that he or she has no objection to their release.

(ii) The source of the information to be released is a public document such as commercial telephone directory or other public listing.

(iii) The release is required by Federal statute (for example, pursuant to Federally-funded state programs to locate parents who have defaulted on child support payments (42 U.S.C. section 653).)

(iv) The releasing official releases the information under the provisions of DLAR 5400.14, (32 CFR part 1285).

(5) Records may be disclosed outside DoD without consent of the individual to whom they pertain for an established routine use. Routine uses may be established, discontinued, or amended without the consent of the individuals involved. However, new or changed routine uses must be published in the FEDERAL REGISTER at least 30 days before actually disclosing any records under their provisions. In addition to the routine uses established by the individual system notices, common blanket routine uses for all DLA-maintained systems of records have been established. These blanket routine uses are published in DLAH 5400.1,[1] DLA Systems of Records Handbook. Unless a system notice specifically excludes a system from a given blanket routine use, all blanket routine uses apply.

(6) Records in DLA systems of records may be disclosed without the consent of the individuals to whom they pertain to the Bureau of the Census for purposes of planning or carrying out a census survey or related activities.

(7) Records may be disclosed for statistical research and reporting without the consent of the individuals to whom they pertain. Before such disclosures, the recipient must provide advance written assurance that the records will be used as statistical research or reporting records; the records will only be transferred in a form that is not individually identifiable; and the records will not be used, in whole or in part, to make any determination about the rights, benefits, or entitlements of specific individuals. A disclosure accounting is not required.

(8) Records may be disclosed without the consent of the individual to whom they pertain to the National Archives and Records Administration (NARA) if they have historical or other value to warrant continued preservation; or for evaluation by NARA to determine if a record has such historical or other value. Records transferred to a Federal Record Center (FRC) for safekeeping and storage do not fall within this category. These remain under the control of the transferring activity, and the FRC personnel are considered agents of the activity which retain control over the records. No disclosure accounting is required for the transfer of records to FRCs.

(9) Records may be disclosed without the consent of the individual to whom they pertain to another agency or an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity, provided the civil or criminal law enforcement activity is authorized by law; the head of the law enforcement acitivity or a designee has made a written request specifying the particular records desired and the law enforcement purpose (such as criminal investigations, enforcement of civil law, or a similar propose) for which the record is sought; and there is no Federal statute that prohibits the disclosure of the records. Normally, blanket requests for access to any and all records pertaining to an individual are not honored. When a record is released to a law enforcement activity, maintain a disclosure accounting. This disclosure accounting will not be made available to the individual to whom the record pertains if the law enforcement activity requests that the disclosure not be released.

(10) Records may be disclosed without the consent of the individual to whom they pertain if disclosure is made under compelling circumstances affecting the health or safety of any individual. The affected individual need not be the subject of the record disclosed. When such a disclosure is made, notify the individual who is the subject of the record. Notification sent to the

[1] Copies may be obtained from the Defense Logistics Agency, ATTN: DSS-CV, 8725 John J. Kingman Road, Suite 2533, Fort Belvoir, VA 22060–6221.

last known address of the individual as reflected in the records is sufficient.

(11) Records may be disclosed without the consent of the individual to whom they pertain to either House of the Congress or to any committee, joint committee or subcommittee of Congress if the release pertains to a matter within the jurisdiction of the committee. Records may also be disclosed to the General Accounting Office (GAO) in the course of the activities of GAO.

(12) Records may be disclosed without the consent of the person to whom they pertain under a court order signed by a judge of a court of competent jurisdiction. Releases may also be made under the compulsory legal process of Federal or state bodies having authority to issue such process.

(i) When a record is disclosed under this provision, make reasonable efforts to notify the individual to whom the record pertains, if the legal process is a matter of public record.

(ii) If the process is not a matter of public record at the time it is issued, seek to be advised when the process is made public and make reasonable efforts to notify the individual at that time.

(iii) Notification sent to the last known address of the individual as reflected in the records is considered reasonable effort to notify. Make a disclosure accounting each time a record is disclosed under a court order or compulsory legal process.

(13) Certain personal information may be disclosed to consumer reporting agencies as defined by the Federal Claims Collection Act. Information which may be disclosed to a consumer reporting agency includes:

(i) Name, address, taxpayer identification number (SSN), and other information necessary to establish the identity of the individual.

(ii) The amount, status, and history of the claim.

(iii) The agency or program under which the claim arose.

(g) *Disclosure accounting.* (1) Keep an accurate record of all disclosures made from any system of records except disclosures to DoD personnel for use in the performance of their official duties or under DLAR 5400.14 (32 CFR part 1285). In all other cases a disclosure accounting is required even if the individual has consented to the disclosure of the information pertaining to him or her.

(2) Use any system of disclosure accounting that will provide the necessary disclosure information. As a minimum, disclosure accounting will contain the date of the disclosure, a description of the information released, the purpose of the disclosure, the name and address of the person or agency to whom the disclosure was made. When numerous similar records are released (such as transmittal of payroll checks to a bank), identify the category of records disclosed and include the data required in some form that can be used to construct an accounting disclosure record for individual records if required. Retain disclosure accounting records for 5 years after the disclosure or the life of the record, whichever is longer.

(3) Make available to the individual to whom the record pertains all disclosure accountings except when the disclosure has been made to a law enforcement activity and the law enforcement activity has requested that disclosure not be made, or the system of records has been exempted from the requirement to furnish the disclosure accounting. If disclosure accountings are not maintained with the record and the individual requests access to the accounting, prepare a listing of all disclosures and provide this to the individual upon request.

(h) *Collecting personal information.* (1) Collect to the greatest extent practicable personal information directly from the individual to whom it pertains if the information may be used in making any determination about the rights, privileges, or benefits of the individual under any Federal program.

(2) When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, a Privacy Act Statement is required regardless of the medium used to collect the information (forms, personal interviews, stylized formats, telephonic interviews, or other methods). The statement enables

the individual to make an informed decision whether to provide the information requested. If the personal information solicited is not to be incorporated into a system of records, the statement need not be given. The Privacy Act Statement shall be concise, current, and easily understood. It must include:

(i) The specific Federal statute or Executive Order that authorizes collection of the requested information.

(ii) The principal purpose or purposes for which the information is to be used.

(iii) The routine uses that will be made of the information.

(iv) Whether providing the information is voluntary or mandatory.

(v) The effects on the individual if he or she chooses not to provide the requested information.

(3) The Privacy Act Statement may appear as a public notice (sign or poster), conspicuously displayed in the area where the information is collected, such as at check-cashing facilities or identification photograph facilities. The individual normally is not required to sign the Privacy Act Statement. Provide the individual a written copy of the Privacy Act Statement upon request. This must be done regardless of the method chosen to furnish the initial advisement.

(4) Include in the Privacy Act Statement specifically whether furnishing the requested personal data is mandatory or voluntary. A requirement to furnish personal data is mandatory only when a Federal statute, Executive order, regulation, or other lawful order specifically imposes a duty on the individual to provide the information sought, and the individual is subject to a penalty if he or she fails to provide the requested information. If providing the information is only a condition of a prerequisite to granting a benefit or privilege and the individual has the option of requesting the benefit or privilege, providing the information is always voluntary. However, the loss or denial of the privilege, benefit, or entitlement sought may be listed as a consequence of not furnishing the requested information.

(5) It is unlawful for any Federal, state, or local government agency to deny an individual any right, benefit, or privilege provided by law because the individual refuses to provide his or her social security number (SSN). However, if a Federal statute requires that the SSN be furnished or if the SSN is required to verify the identity of the individual in a system of records that was established and in use before January 1, 1975, and the SSN was required as an identifier by a statute or regulation adopted before that date, this restriction does not apply.

(i) When an individual is requested to provide his or her SSN, he or she must be told:

(A) The uses that will be made of the SSN.

(B) The statute, regulation, or rule authorizing the solicitation of the SSN.

(C) Whether providing the SSN is voluntary or mandatory.

(ii) Include in any systems notice for any system of records that contains SSNs a statement indicating the authority for maintaining the SSN and the source of the SSNs in the system. If the SSN is obtained directly from the individual indicate whether this is voluntary or mandatory.

(iii) Upon entrance into Military Service of civilian employment with DoD, individuals are asked to provide their SSNs. The SSN becomes the service or employment number for the individual and is used to establish personnel, financial, medical, and other official records. After an individual has provided his or her SSN for the purpose of establishing a record, a Privacy Act Statement is not required if the individual is only requested to furnish or verify the SSNs for identification purposes in connection with the normal use of his or her records. However, if the SSN is to be written down and retained for any purpose by the requesting official, the individual must be provided a Privacy Act Statement.

(6) DLAI 5530.1, Publications, Forms, Printing, Duplicating, Micropublishing, Office Copying, and Automated Information Management Programs,[2] provides guidance on administrative

[2] Copies may be obtained from the Defense Logistics Agency, ATTN: DSS-CV, 8725 John J. Kingman Road, Suite 2533, Fort Belvoir, VA 22060–6221.

requirements for Privacy Act Statements used with DLA forms. Forms subject to the Privacy Act issued by other Federal agencies have a Privacy Act Statement attached or included. Always ensure that the statement prepared by the originating agency is adequate for the purpose for which the form will be used by the DoD activity. If the Privacy Act Statement provided is inadequate, the activity concerned will prepare a new statement of a supplement to the existing statement before using the form. Forms issued by agencies not subject to the Privacy Act (state, municipal, and other local agencies) do not contain Privacy Act Statements. Before using a form prepared by such agencies to collect personal data subject to this part, an appropriate Privacy Act Statement must be added.

(i) *Systems of records.* (1) To be subject to this part, a ''system of records'' must consist of records retrieved by the name of an individual or some other personal identifier and be under the control of a DLA activity. Records in a group of records that *may be* retrieved by a name or personal identifier are not covered by this part. The records *must be*, in fact, retrieved by name or other personal identifier to become a system of records for the purpose of this part.

(2) Retain in a system of records only that personal information which is relevant and necessary to accomplish a purpose required by a Federal statute or an Executive Order. The existence of a statute or Executive order mandating that maintenance of a system of records does not abrogate the responsibility to ensure that the information in the system of records is relevant and necessary.

(3) Do not maintain any records describing how an individual exercises his or her rights guaranteed by the First Amendment of the U.S. Constitution unless expressly authorized by Federal statute or the individual. First Amendment rights include, but are not limited to, freedom of religion, freedom of political beliefs, freedom of speech, freedom of the press, the right to assemble, and the right to petition.

(4) Maintain all personal information used to make any determination about an individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual in making any such determination. Before disseminating any personal information from a system of records to any person outside DoD, other than a Federal agency, make reasonable efforts to ensure that the information to be disclosed is accurate, relevant, timely, and complete for the purpose it is being maintained.

(5) Establish appropriate administrative, technical and physical safeguards to ensure that the records in every system of records are protected from unauthorized alteration or disclosure and that their confidentiality is protected. Protect the records against reasonably anticipated threats or hazards. Tailor safeguards specifically to the vulnerabilities of the system and the type of records in the system, the sensitivity of the personal information stored, the storage medium used and, to a degree, the number of records maintained.

(i) Treat all unclassified records that contain personal information that normally would be withheld from the public as if they were designated ''For Official Use Only'' and safeguard them in accordance with the standards established by DLAR 5400.14 (32 CFR part 1285) even if they are not marked ''For Official Use Only.''

(ii) Special administrative, physical, and technical procedures are required to protect data that are stored or being processed temporarily in an automated data processing (ADP) system or in a word processing activity to protect it against threats unique to those environments (see DLAR 5200.17, Security Requirements for Automated Information and Telecommunications Systems,[3] and appendix D to this part).

(6) Dispose of records containing personal data so as to prevent inadvertent compromise. Disposal methods such as tearing, burning, melting, chemical decomposition, pulping, pulverizing, shredding, or mutilation are considered

[3] Copies may be obtained from the Defense Logistics Agency, ATTN: DSS-CV, 8725 John J. Kingman Road, Suite 2533, Fort Belvoir, VA 22060–6221.

adequate if the personal data is rendered unrecognizable or beyond reconstruction.

(i) The transfer of large quantities of records containing personal data (for example, computer cards and printouts) in bulk to a disposal activity, such as the Defense Property Disposal Office, is not a release of personal information under this part. The sheer volume of such transfers makes it difficult or impossible to identify readily specific individual records.

(ii) When disposing of or destroying large quantities of records containing personal information, care must be exercised to ensure that the bulk of the records is maintained so as prevent specific records from being readily identified. If bulk is maintained, no special procedures are required.

(7) When DLA contracts for the operation or maintenance of a system of records or a portion of a system of records by a contractor, the record system or the portion of the record system affected are considered to be maintained by DLA and are subject to this part. The activity concerned is responsible for applying the requirements of this part to the contractor. The contractor and its employees are to be considered employees of DLA for purposes of the sanction provisions of the Privacy Act during the performance of the contract. See the Federal Acquisition Regulation (FAR), section 24.000 (48 CFR chapter 1).

(j) *System Notices.* (1) A notice of the existence of each system of records must be published in the FEDERAL REGISTER. While system notices are not subject to formal rulemaking procedures, advance public notice must be given before an activity may begin to collect personal information or use a new system of records. The notice procedures require that:

(i) The system notice describes the contents of the record system and the routine uses for which the information in the system may be released.

(ii) The public be given 30 days to comment on any proposed routine uses before implementation.

(iii) The notice contains the date on which the system will become effective.

(2) Appendix A of this part discusses the specific elements required in a system notice. DLAH 5400.1[4] contains systems notices published by DLA.

(3) In addition to system notices, reports are required for new and altered systems of records. The criteria of these reports are outlined in appendixes B and C of this part. No report is required for amendments to existing systems which do not meet the criteria for altered record systems.

(4) System managers shall evaluate the information to be included in each new system before establishing the system and evaluate periodically the information contained in each existing system of records for relevancy and necessity. Such a review will also occur when a system notice amendment or alteration is prepared. Consider the following:

(i) The relationship of each item of information retained and collected to the purpose for which the system is maintained.

(ii) The specific impact on the purpose or mission of not collecting each category of information contained in the system.

(iii) The possibility of meeting the informational requirements through use of information not individually identifiable or through other techniques, such as sampling.

(iv) The length of time each item of personal information must be retained.

(v) The cost of maintaining the information.

(vi) The necessity and relevancy of the information to the purpose for which it was collected.

(5) Systems notices and reports of new and altered systems will be submitted to DLA Support Services (DSS-CA) as required.

(k) *Exemptions.* The Director, DLA will designate the DLA records which are to be exempted from certain provisions of the Privacy Act. DLA Support Services (DSS-CA) will publish in the FEDERAL REGISTER information specifying the name of each designated system, the specific provisions of the Privacy Act from which each system is to

[4] Copies may be obtained from the Defense Logistics Agency, ATTN: DSS-CV, 8725 John J. Kingman Road, Suite 2533, Fort Belvoir, VA 22060–6221.

be exempted, the reasons for each exemption, and the reason for each exemption of the record system.

(1) *General Exemptions*. To qualify for a general exemption, as defined in the Privacy Act, the system of records must be maintained by a system manager who performs as his/her principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities or prosecutors, courts, correctional, probation, pardon, or parole authorities. Such system of records must consist of:

(i) Information compiled for the purpose of identifying individual criminal offenders and alleged offenders and containing only identifying data and notations or arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole, and probation status.

(ii) Information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual.

(iii) Reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

(2) *Specific exemption*. To qualify for a specfic exemption, as defined by the Privacy Act, the systems of records must be:

(i) Specifically authorized under criteria established by an Executive Order to be kept classified in the interest of national defense or foreign policy and are in fact properly classified pursuant to such Executive Order.

(ii) Investigatory material compiled for law enforcement purposes other than material covered under a general exemption. However, an individual will not be denied access to information which has been used to deny him/her a right or privilege unless disclosure would reveal a source who furnished information to the Government under a promise that the identity of the source would be held in confidence. For investigations made after September 27, 1975, the identity of the source may be treated as confidential only if based on the expressed guarantee that the identity would not be revealed.

(iii) Maintained in connection with providing protective services to the President of the United States or other individuals protected pursuant to 18 U.S.C. 3056.

(iv) Used only to generate aggregate statistical data or for other similarly evaluative or analytic purposes, and which are not used to make decisions on the rights, benefits, or entitlements of individuals except for the disclosure of a census record permitted by 13 U.S.C. 8.

(v) Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Military Service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the source would be held in confidence, or prior to September 27 1975, under an implied promise that the identity of the source would be held in confidence.

(vi) Testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service, the disclosure of which would compromise the objectivity or fairness of the testing or elimination process.

(vii) Evaluation material used to determine potential for promotion in the Military Services, but only the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence or prior to September 27, 1975, under an implied promise that the identity of the source would be held in confidence. System managers will specify those categories of individuals for whom pledges of confidentiality may be made when obtaining information on an individual's suitability for promotion.

(viii) Exemption rules for DLA systems of records are published in appendix H of this part.

(l) *Matching Program Procedures*. The OMB has issued special guidelines to be

followed in programs that match the personal records in the computerized data bases of two or more Federal agencies by computer (see appendix E). These guidelines are intended to strike a balance between the interest of the Government in maintaining the integrity of Federal programs and the need to protect individual privacy expectations. They do not authorize matching programs as such and each matching program must be justified individually in accordance with the OMB guidelines.

(1) Forward all requests for matching programs to include necessary routine use amendments and analysis and proposed matching program reports to DLA Support Services. Changes to existing matching programs shall be processed in the same manner as a new matching program report.

(2) No time limits are set by the OMB guidelines. However, in order to establish a new routine use for a matching program, the amended system notice must have been published in the FEDERAL REGISTER at least 30 days before implementation. Submit the documentation required above to DLA Support Services (DSS-CA) at least 60 days before the proposed initiation date of the matching program. Waivers to the 60 days' deadline may be granted for good cause shown. Requests for waivers will be in writing a fully justified.

(3) For the purpose of the OMB guidelines, DoD and all DoD Components are considered a single agency. Before initiating a matching program using only the records of two or more DoD activities, notify DLA Support Services (DSS-CA) that the match is to occur. Further information may be requested from the activity proposing the match.

(4) System managers shall review annually each system of records to determine if records from the system are being used in matching programs and whether the OMB Guidelines have been complied with.

[DLAR 5400.21, 51 FR 33595, Sept. 22, 1986, unless otherwise noted. Redesignated at 56 FR 57803, Nov. 14, 1991, as amended at 66 FR 41781, Aug. 9, 2001.

§ 323.6 Forms and reports.

DLA activities may be required to provide data under reporting requirements established by the Defense Privacy Office and DLA Support Services (DSS-CA). Any report established shall be assigned Report Control Symbol DD-DA&M(A)1379.

[66 FR 41782, Aug. 9, 2001]

APPENDIX A TO PART 323—INSTRUCTIONS FOR PREPARATION OF SYSTEM NOTICES

A. *System identification*. See DLAH 5400.1.[1]

B. *System name*. The name of the system reasonably identifies the general purpose of the system and, if possible, the general categories of individuals involved. Use acronyms only parenthetically following the title or any portion thereof, such as, ''Joint Uniform Military Pay System (JUMPS).'' Do not use acronyms that are not commonly known unless they are preceded by an explanation. The system name may not exceed 55 character positions including punctuation and spacing.

C. *System location* 1. For systems maintained in a single location provided the exact office name, organizational identity, and address or routing symbol. For geographically or organizationally decentralized systems, specify each level of organization or element that maintains a segment of the system. For automated data systems with a central computer facility and input/output terminals at several geographically separated location, list each location by category.

2. When multiple locations are identified by type of organization, the system location may indicate that official mailing addresses are contained in an address directory published as an appendix to DLAH 5400.1.

3. If no address directory is used or the addresses in the directory are incomplete, the address of each location where a segment of the record system is maintained must appear under the ''System Location'' caption. Classified addresses are not listed, but the fact that they are classified is indicated. Use the standard U.S. Postal Service two letter state abbreviation symbols and zip codes for all domestic addresses.

D. *Categories of individuals covered by the system*. Set forth the specific categories of individuals to whom records in the system pertain in clear, easily understood, nontechnical terms. Avoid the use of broad over-general descriptions, such as ''all DLA personnel'' or ''all civilian personnel'' unless this actually reflects the category of individuals involved.

E. *Categories of records in the system*. Describe in clear, nontechnical terms the types

[1] Copies may be obtained from the Defense Logistics Agency, ATTN: DSS-CV, 8725 John J. Kingman Road, Suite 2533, Fort Belvoir, VA 22060–6221.

[2] [Reserved]